James E. Cecchi, Esq.
CARELLA BYRNE CECCHI
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
T: (973) 994-1700
jcecchi@carellabyrne.com

Counsel for Plaintiff
[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

LONNY DAVID MATLICK, D.B.A. LONNY D. MATLICK D.O., individually and on behalf of all others similarly situated, Plaintiff, v. CHANGE HEALTHCARE INC., OPTUM, INC., and UNITEDHEALTH GROUP INCORPORATED, Defendants.	Civil Action No: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Lonny David Matlick, M.D., d.b.a. Lonny D. Matlick D.O.,[1] by and through its attorneys, brings this class action complaint against defendants Change Healthcare Inc. ("Change Healthcare"), Optum, Inc. ("Optum") and UnitedHealth

[1] This Complaint refers to Plaintiff as his dba, Lonny D. Matlick D.O.

Group Incorporated ("UnitedHealth") (collectively, "Defendants") on behalf of itself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to its own actions and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. Plaintiff brings this proposed class action against Defendants for their failure to maintain the security of their computer networks in accordance with state and federal law.

2. Defendant Change Healthcare – a unit of UnitedHealth's Optum subsidiary – is a healthcare company that provides revenue and payment cycle management services that lie at the heart of the U.S. healthcare system. Change Healthcare's services connect payers, providers, pharmacies, and patients. The services are critical to providing healthcare throughout the country.

3. Defendants' computer networks include data processing systems, portals, and platforms that provide critical infrastructure for administering healthcare across the United States. Defendants' services to healthcare providers and pharmacies include clearinghouse services, which allow providers to submit electronic claims to insurance companies and facilitate the electronic payments from insurance companies to providers.

4. Change Healthcare processes 15 billion transactions annually, touching one in three U.S. patient records, and is used by over a million healthcare providers, including hospitals, physicians, therapists, pharmacies, and laboratories.

5. Given their role in providing the infrastructure in the nationwide delivery of healthcare, Defendants knew they needed to implement effective cybersecurity controls to prevent foreseeable disruptions and protect the highly sensitive personal and healthcare information entrusted to Defendants.

6. On February 21, 2024, UnitedHealth announced that "a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems"[2] (the "Data Breach"). After detecting the Data Breach, UnitedHealth claimed to have "proactively isolated the impacted systems from mother connecting systems."[3] UnitedHealth also said it was "working with law enforcement" and allegedly "notified customers, clients and certain government agencies" of the breach.[4]

7. On February 28, 2024, UnitedHealth announced that the cyberattack at its tech unit, Change Healthcare, was perpetrated by hackers who identified

[2] UnitedHealth Group Incorporation Form 8-K, filed with the SEC on Feb. 21, 2024, *available at* https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.
[3] *Id.*
[4] *Id.*

themselves as the "Blackcat" ransomware group.[5] In a message posted on its darknet site that was quickly deleted, the group known as "Blackcat" or "ALPHV" said it stole millions of sensitive records, including medical insurance and health data, from the company.[6] Pharmacy, medical claims, and payment systems were targeted by the attack.

8. The Data Breach exposed the vulnerabilities in Defendants' computer networks, and as a result, Defendants took all the affected computer networks offline, including the Change Healthcare platform ("Change Platform"). This platform provides, among other things, a revenue and payment cycle management service that connects payers, providers, and patients within the U.S. healthcare system.[7] The Change Platform is widely used among practitioners. Without the Change Platform, the U.S. healthcare industry is immobilized.

9. Since the Data Breach was discovered on February 21, 2024, healthcare providers and healthcare service providers have been unable to get paid on claims for medical treatment and services they have provided.

---

[5] *See UnitedHealth says 'Blackcat' ransomware group behind hack at tech unit,* REUTERS (Feb. 29, 2024,) *available at* https://www.reuters.com/technology/unitedhealth-confirms-blackcat-group-behind-recent-cyber-security-attack-2024-02-29/.

[6] *Id*.

[7] *See Revenue Cycle Management*, CHANGE HEALTHCARE, *available at* https://www.changehealthcare.com/revenue-cycle-management.

10. The American Hospital Association ("AHA") has described the effects of the Data Breach as a "staggering loss of revenue."[8] The Data Breach is estimated to be "costing some providers over $100 million a day."[9]

11. The ripple effect of the Data Breach is not only affecting patients; it is also hampering healthcare providers' practices. According to John Riggi, national advisor for cybersecurity and risk at the AHA, the "cyberattack has affected every hospital in the country one way or another."[10] Many providers are having trouble verifying patient eligibility and coverage, filing claims, and billing patients.[11] This leaves small and mid-sized practices especially vulnerable without normal cash flow to sustain operations. Since the Data Breach, healthcare practices and service providers have received little, if any, reimbursement from insurers. Without these reimbursements, small and mid-sized practices cannot afford employee payroll, rent/mortgage, and medical supplies.

12. On March 13, 2024, the U.S. Department of Health and Human Services ("HHS") said Wednesday it has begun an investigation into the incident.[12]

---

[8] *See AHA Urges More Congressional Action to Help Providers Affected By Change Healthcare Cyberattack* (Mar. 13, 2024), *available at* https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack.
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *HHS Office of Human Rights Issues Letter and Opens Investigation of Change Healthcare Cyberattack*, HHS PRESS OFFICE (Mar. 13. 2024), *available at* https://www.hhs.gov/about/news/2024/03/13/hhs-office-civil-rights-issues-letter-opens-investigation-change-healthcare-cyberattack.html.

The HHS Office for Civil Rights ("OCR") said it plans to focus on assessing the extent of the breach and whether UnitedHealth Group and its affected subsidiary, Change Healthcare, took adequate steps to protect patient data under the Health Insurance Portability and Accountability Act ("HIPAA").

13. The healthcare industry has been a target of cyberattacks for years given the massive amount of confidential personal health information ("PHI") and personal identifying information ("PII") that healthcare organizations collect, store, and maintain and that can be used to commit identity theft. Ransomware and hacking are the primary cyber-threats in health care.[13] Over the past five years, there has been a 256% increase in large breaches reported to OCR involving hacking and a 264% increase in ransomware. In 2023, hacking accounted for 79% of the large breaches reported to OCR. The large breaches reported in 2023 affected over 134 million individuals, a 141% increase from 2022.

14. Furthermore, on December 19, 2023, the Federal Bureau of Investigation ("FBI"), the Cybersecurity and Infrastructure Security Agency ("CISA"), and the HHS issued a joint cyber security advisory warning businesses in the healthcare sector that since mid-December 2023, ALPHV Blackcat ransomware has targeted the healthcare sector and encouraging critical infrastructure organizations, such as Defendants, to implement the recommendations set forth in

[13] *Id.*

the advisory to reduce the likelihood and impact of inevitable ALPHV Blackcat ransomware and data extortion efforts.[14] The joint cyber security advisory provided technical details associated with the ALPHV Blackcat criminal organization and its attack techniques, and advised organizations of "actions to take today," which included "prioritize remediation of known exploited vulnerabilities."[15]

15. Notwithstanding these publicized high-priority, emergent, and critical warnings, Defendants failed to take reasonable, timely, and appropriate measures to protect against the Data Breach. The Data Breach and related shutdown were entirely foreseeable and could have been avoided.

16. Plaintiff and the proposed Class Members are healthcare businesses that were injured as a result of the disruption to Defendants' insurance claims clearinghouse, Defendants' failure to timely and adequately process and pay amounts due and owing to Plaintiff and Class Members for the healthcare services and products, and other financial loss caused by the disruption to Defendants' networks and transactional services. Plaintiffs and Class members seek damages and injunctive relief for the injuries they sustained as a result of the Data Breach, which continues to negatively impact their businesses.

[14] *Joint Cybersecurity Advisory: #StopRansomware: ALPHV Blackcat* (Dec. 19, 2023), *available at* https://aspr.hhs.gov/cyber/Documents/stopransomware-508.pdf.
[15] *Id*.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 putative members in the proposed class, and Plaintiff and Defendants are diverse parties.

18. The Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged are part of the same case or controversy.

19. This Court has personal jurisdiction over Defendants. Defendant Change Healthcare is headquartered and routinely conducts business in the State where this District is located. Each of the Defendants have sufficient minimum contacts in this State, have intentionally availed themselves of this jurisdiction by conducting business in this State, including through marketing and/or selling products and/or services and/or by accepting and processing payments for those products and/or services within this State.

20. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within this District, and Defendants regularly conduct business in this District.

THE PARTIES

21. Plaintiff Lonny D. Matlick, D.O. is a sole proprietorship, with a primary business address of 2306 New Road, Northfield, New Jersey. Plaintiff is a healthcare provider specializing in otolaryngology.

22. Defendant Change Healthcare is incorporated in Delaware and is headquartered in Nashville, Tennessee. It became a subsidiary of UnitedHealth in 2022 and is operated by UnitedHealth's subsidiary, Optum.

23. Defendant Optum is incorporated in Delaware and is headquartered in Eden Prairie, Minnesota. Optum is a subsidiary of UnitedHealth that offers healthcare services, including technology and related services, pharmacy care services and various direct healthcare services.

24. Defendant UnitedHealth is incorporated in Delaware and is headquartered in Minnetonka, Minnesota. UnitedHealth exercises control over the management of Optum and the Change Healthcare cybersecurity systems as evidenced by UnitedHealth's response to the Data Breach as alleged herein.

FACTUAL ALLEGATIONS

A. Background

25. Change Healthcare is a healthcare technology company that works across the U.S. health system "to make clinical, administrative and financial processes simpler and more efficient for payers, providers, and consumers."

26. Change Healthcare operates the nation's largest electronic data interchange clearinghouse, which transmits data between healthcare providers and insurers, allowing them to exchange insurance claims, remittances, and other healthcare-related transactions. Approximately 50 percent of all medical claims in the United States pass through Change Healthcare's electronic data interchange clearinghouse.

27. Change Healthcare offers healthcare providers such as doctors, hospitals, therapists, pharmacies, laboratories, and clinics, services and support in key areas such as provider claim processing, pharmacy claim transactions, verification of insurance, disbursement of provider payments, and authorizations and medical necessity reviews. Healthcare providers utilize Change Healthcare's services either through a direct contractual relationship or indirectly through third-party intermediaries.

28. According to Change Healthcare's website, its "extensive network, innovative technology, and expertise inspire a stronger, better coordinated, increasingly collaborative, and more efficient healthcare system." It bills itself as a "trusted partner for organizations committed to improving the healthcare system through technology."

29. In the regular course of business, Change Healthcare collects and stores patients' highly sensitive health information collected from its clients like Medicare,

pharmacies, healthcare providers, and other healthcare-related entities. Examples of the personal information Change Healthcare maintains include patients' full names, phone numbers, addresses, Social Security numbers, emails, medical records, dental records, payment information, claims information, insurance records, and the like.

30. Change Healthcare recognizes in its Code of Conduct that it "has an obligation to safeguard information … about the companies with which we do business."[16] Change Healthcare further recognizes that its customers "trust us to respect and protect personally identifiable (PI) and other sensitive information," and "PI is protected under various federal, state, and other international privacy, security, healthcare, credit and financial laws. We collect, store, access, use, share, store, transfer and dispose of PI responsibly."[17] Change Healthcare further states that it "respect(s) and protect(s) the sensitive nature of PHI and carefully maintain(s) its confidentiality."[18]

31. Given Change Healthcare's representations concerning its obligations to protect the highly sensitive PI and PHI it collects, stores and maintains, Change Healthcare understood the need for it to protect PI and PHI and prioritize data security.

---

[16] The Integrity of Change, Our Code of Conduct, Change Healthcare, *available at* https://codeofconduct.changehealthcare.com/?adobe_mc=MCORGID%3D26CD3A665C7D19990A495D73%2540AdobeOrg%7CTS%3D1711401713.
[17] *Id.*
[18] *Id.*

B. The Data Breach

32. On February 21, 2024, Defendants discovered the Data Breach and that their computer networks were not secure and could not protect PHI and PII as required by state and federal law. UnitedHealth set up a page on its website, www.unitedhealthgroup.com, to announce the Data Breach and stated that it disconnected the Change Healthcare systems.[19] UnitedHealth also disclosed the announcement in a filing with the SEC on February 21, 2024.[20] UnitedHealth also stated, "The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies . . . At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational."[21]

33. On February 29, 2024, UnitedHealth confirmed that the ransomware group Blackcat was behind the cyberattack. In a since-deleted post on the dark web, Blackcat said on February 28, 2024, that it was behind the attack on Change Healthcare's systems.[22] The group said it managed to extract six terabytes of data,

[19] *See* https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html.
[20] UnitedHealth Group Incorporation Form 8-K, filed with the SEC on Feb. 21, 2024, *available at* https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm.
[21] *Id*.
[22] *Ransomware group Blackcat is behind cyberattack at UnitedHealth division, company says*, CNBC (Feb. 29, 2024), *available at* https://www.cnbc.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html.

including information like medical records, insurance records, and payment information.[23]

34. On March 7, 2024, UnitedHealth said in a statement: "We are working aggressively on the restoration of our systems and services."[24] UnitedHealth also stated, "All of us at UnitedHealth Group feel a deep sense of responsibility for recovery and are working tirelessly to ensure that providers can care for their patients and run their practices, and that patients can get their medications. We're determined to make this right as fast as possible."[25]

35. Following the Data Breach, the AHA issued a "Cybersecurity Advisory" in which it encouraged health care organizations that may have been exposed to the data breach to "disconnect[] from applications specified by Change Healthcare that remain unavailable due to this cyberattack."[26] The AHA also notified the public that "**Change Healthcare has not provided a specific timeframe for which recovery of the impacted applications is expected.**"[27] The AHA further recognized that "hospitals and health systems may be experiencing

[23] *Id*.
[24] *UnitedHealth Group Update on Change Healthcare Cyberattack* (Mar. 7, 2024), *available at* https://www.unitedhealthgroup.com/newsroom/2024/2024-03-07-uhg-update-change-healthcare-cyberattack.html.
[25] *Id*.
[26] *Update: UnitedHealth Group's Change Healthcare's Continued Cyberattack Impacting Health Care Providers*, AHA CYBER SECURITY ADVISORY (Feb. 24, 2024), *available at* https://www.aha.org/2024-02-24-update-unitedhealth-groups-change-healthcares-continued-cyberattack-impacting-health-care-providers.
[27] *Id*. (Emphasis in original.)

challenges with obtaining care authorizations for their patients, as well as delays in payment."[28] The AHA further stated it was "communication with the Department of Health and Human Services, including the Centers for Medicare & Medicaid Services, about options to support patients' timely access to care and provide temporary financial support to providers."[29]

36. In a letter to HHS on February 26, 2024, the AHA stated that while the full scope was "unknown," the AHA expected impacts to be far-reaching given Change Healthcare's national presence.[30] The AHA also explained how the Data Breach has affected healthcare providers in terms of being unable to collect revenue: "without this critical revenue source, hospitals and health systems may be unable to pay salaries for clinicians and other members of the care team, acquire necessary medicines and supplies, and pay for mission critical contract work in areas such as physical security, dietary and environmental services."[31] "In addition, replacing previously electronic processes with manual processes will add considerable administrative costs on providers, as well as divert team members from other tasks. It is particularly concerning that while Change Healthcare's systems remain

[28] *Id*.
[29] *Id*.
[30] AHA Letter to HHS on Implications of Change Healthcare Cyberattack, AMERICAN HOSPITAL ASSOCIATION (Feb. 26, 2024), *available at* https://www.aha.org/lettercomment/2024-02-26-aha-letter-hhs-implications-change-healthcare-cyberattack.
[31] *Id*.

disconnected, it and its parent entities benefit financially, including by accruing interest on potentially billions of dollars that belong to health care providers."[32]

C. The Data Breach and Shutdown of Change Healthcare's Systems Have Imposed Significant Consequences on Healthcare Providers, Including Staggering Revenue Losses

37. Thousands of healthcare providers across the country have been severely impacted by the Data Breach.

38. When Change Healthcare disconnected its platform, many healthcare providers lost their primary – or only –source of processing payments for their services through patients' healthcare plans and thus are not receiving payment. Healthcare providers and healthcare service providers are absorbing these upfront costs.

39. According to a survey by the AHA, "more than 80% of hospitals said the cyberattack has affected their cash flow, and of those nearly 60% report that the impact to revenue is $1 million per day or more. In addition, the survey found that 74% of hospitals reported impacts to direct patient care as a result of the cyberattack."[33]

---

[32] *Id*.

[33] *AHA Survey: Change Healthcare cyberattack having significant disruptions on patient care, hospitals' finances*, AMERICAN HOSPITAL ASSOCIATION (Mar. 15, 2024), *available at* https://www.aha.org/news/news/2024-03-15-aha-survey-change-healthcare-cyberattack-having-significant-disruptions-patient-care-hospitals-finances.

40. Small private practices and health-care providers are also facing mounting financial pressures as crucial reimbursement systems through Change Healthcare's platform remain down following the Data Breach.[34] In addition to disrupting patient care, the Data Breach has impacted providers' ability to receive reimbursements from insurers, effectively grinding many health systems' revenue cycles to a halt.[35] "Smaller and mid-sized practices that rely on reimbursement cash flow to operate are making tough decisions about how to stay afloat. If the outage drags on for too long, experts say some practices may have to close their doors for good."[36]

41. On March 13, 2024, the AHA wrote to Senators Ron Wyden and Mike Crapo about the Data Breach, stating that the downed systems "are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process."[37] In addition, hospitals, health systems and other providers

[34] *Outages from Change Healthcare cyberattack causing financial 'mess' for doctors*, CNBC (Feb. 29, 2024), *available at* https://www.cnbc.com/2024/02/29/change-healthcare-cyberattack-has-caused-financial-mess-for-doctors.html.
[35] *Id*.
[36] *Id*.
[37] *AHA Urges More Congressional Action to Help Providers Affected By Change Healthcare Cyberattack*, AMERICAN HOSPITAL ASSOCIATION (Mar. 13, 2024), *available at*

are experiencing extraordinary reductions in cash flow, threatening their ability to make payroll and to acquire the medical supplies needed to provide care.[38]

42. On March 13, 2024, the AHA wrote to Senators Ron Wyden and Mike Crapo about the Data Breach, stating that the downed systems "are hampering providers' ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, and in some instances, access the clinical guidelines used in clinical decision support tools and as part of the prior authorization process."[39] In addition, hospitals, health systems and other providers are experiencing extraordinary reductions in cash flow, threatening their ability to make payroll and to acquire the medical supplies needed to provide care.[40]

D. The Data Breach Was a Known and Foreseeable Risk that Could Have Been Prevented with Reasonable Care

43. Since at least 2018, cybersecurity incidents are a growing threat to the healthcare industry in general.[41]

---

https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack.

[38] *Id*.

[39] *AHA Urges More Congressional Action to Help Providers Affected By Change Healthcare Cyberattack*, AMERICAN HOSPITAL ASSOCIATION (Mar. 13, 2024), *available at* https://www.aha.org/lettercomment/2024-03-13-aha-urges-more-congressional-action-help-providers-affected-change-healthcare-cyberattack.

[40] *Id*.

[41] *Cybersecurity in Hospitals: A Systematic Organizational Perspective*, NATIONAL LIBRARY OF MEDICINE (May 28, 2018), *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/.

44. And as recent as December 19, 2023, the FBI, CISA and HHS issued a joint cyber security advisory warning businesses in the healthcare sector that since mid-December 2023, ALPHV Blackcat ransomware has targeted the healthcare sector and detailing various ransomware variants and ransomware threat actors.[42] The cyber security advisory also included recently and historically observed tactics, techniques, and procedures and indicators of compromise to help organizations protect against ransomware.[43] The cyber security advisory also encouraged critical infrastructure organizations, such as Defendants, to implement the recommendations in the advisory to reduce the likelihood and impact of ALPHV Blackcat ransomware and data extortion incidents.[44]

45. Notwithstanding these publicized high-priority, emergent, and critical warnings, Defendants failed to take reasonable, timely and appropriate measures to protect against the Data Breach.

46. Furthermore, this is not the first time that a UnitedHealth related entity has experienced a data breach. On December 29, 2022, United Healthcare discovered its broker platform may be exposed in a way that released customer

[42] *Joint Cybersecurity Advisory: #StopRansomware: ALPHV Blackcat* (Dec. 19, 2023), *available at* https://aspr.hhs.gov/cyber/Documents/stopransomware-508.pdf.
[43] *Id.*
[44] *Id.*

information and enabled users to access parts of the business.[45] On February 3, 2023, the company confirmed an unauthorized user accessed information from its broker and agent portal, including consumers' sensitive information, which includes their names, dates of birth, genders, addresses, Social Security numbers, UHC member ID numbers, Medicare ID numbers, Medicare plan information, and primary care provider information. Upon completing its investigation, UHC began sending out data breach notification letters to all individuals whose information was affected by the recent data security incident.

47. Accordingly, given the industry warnings, prior data breach and the vast amount of PPI and PHI collected, stored and transmitted on Change Healthcare's systems, Defendants knew that they were a target for cybercriminals and should have taken all reasonable steps to avoid cyberattacks. Defendants' failure to heed warnings by the FBI, CISA and HHS and failure to adequately maintain and protect the security of their computer networks resulted in the Data Breach and shutdown and caused harm to Plaintiff and the Class Members.

[45] *See United Healthcare Patients Exposed in An Unexpected Data Breach*, ID STRONG (Sept. 2, 2023), *available at* https://www.idstrong.com/sentinel/unitedhealthcare-patients-exposed-in-data-breach/.

E. Allegations Relating to Plaintiff Lonny D. Matlick D.O.

48. Plaintiff Lonny D. Matlick D.O. is a sole proprietorship located in Northfield, New Jersey.

49. Lonny David Matlick, M.D., a resident of New Jersey, is Plaintiff's sole medical provider who specializes in otolaryngology.

50. As a small private practice, Plaintiff depends on the timely processing of public and private insurance claims to operate. The majority of Plaintiff's charges for medical services provided to its patients are paid for through insurances. The funds Plaintiff receives through insurance payments are critical to Plaintiff's business and are used to pay for its basic operating expenses, including payroll, supplies, and other expenses.

51. Plaintiff does its billing through a third-party, CareCloud, which processes Plaintiff's patients' insurance claims and submits them to Change Healthcare. Plaintiff is then reimbursed for services by the responsible insurers directly either by direct deposit or checks by mail. Plaintiff pays CareCloud for its services.

52. Since on or about March 10, 2024, Plaintiff's insurance payment collectibles have diminished by 90 percent, and since on or about February 26, 2024, Plaintiff's insurance payment collectibles have diminished by approximately 70 percent.

53. Prior to February 2024, and based upon Plaintiff's 2023 insurance collections, Plaintiff typically collected an average of $9,000 per week in insurance payments. Now, in the two weeks since approximately March 12, 2024, Plaintiff has received a total of less than $500 in insurance payments. As a result, Plaintiff has had to add capital to its business twice in the past month just to maintain its operations – for the first time in the past 16 years.

54. The Data Breach and shutdown have significantly and negatively impacted Plaintiff, whose profits and losses show net income at -34.7% year to date when compared to 2023.

55. Plaintiff presently has no current information on the status of the recovery of Change Healthcare's platform, and it has no indication if and when its cash flow will resume. While Defendants have not provided any information directly to Plaintiff, Plaintiff believes and understands that its inability to receive insurance payments and process patients' insurance claims is the direct and proximate result of Defendants' failure to maintain the security of their computer networks.

F. Defendants Failed to Comply with Federal Law and Regulations Designed to Safeguard Sensitive Health Information

56. Change Healthcare is covered by HIPAA, 45 C.F.R. § 160.102, and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of

Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

57. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider.[46]

58. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[47]

59. HIPAA requires Change Healthcare to implement appropriate safeguards for this information.[48]

60. HIPAA requires Change Healthcare to provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons, *i.e.,* non-encrypted data.[49]

[46] 45 C.F.R. § 160.103.
[47] 45 C.F.R. §164.502.
[48] 45 C.F.R. §164.530(c)(1).
[49] 45 C.F.R. §164.404; §164.402.

61. Change Healthcare acknowledges and discloses in its Privacy Notice that it is a HIPPA covered entity:

> Change Healthcare functions as a HIPAA business associate for its HIPAA covered entity payer and provider customers as its primary business function, so Change Healthcare's collection, use and disclosure of protected health information is guided by HIPAA and the terms of a business associate agreement and other contracts.[50]

62. Change Healthcare acknowledges its obligations under HIPAA, and discloses the Privacy and Security Rules defined by HHS to implement HIPAA requirements:

> Privacy and Security Rules, defined by the Department of Health and Human Services (HHS) to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), address the use, disclosure, and privacy rights of individuals' protected health information (PHI) and security standards for protecting certain health information that is held or transferred in electronic form (e-PHI).
>
> Privacy and Security Rules apply to HIPAA covered entities and contracted business associates which transmit health information in electronic form in connection with a transaction for which the Secretary of HHS has adopted standards under HIPAA.[51]

63. Change Healthcare also states that it takes security measures to safeguard the data it processes:

> We implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or

[50] Change Healthcare Privacy Notice, *available at* https://www.changehealthcare.com/privacy-notice.
[51] Change Healthcare, HIPAA Simplified, Privacy and Security, *available at* https://support.changehealthcare.com/customer-resources/hipaa-simplified/privacy-security.

> misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information. We evaluate and update these measures on an ongoing basis.[52]

64. Despite these requirements, Change Healthcare failed to comply with its duties under HIPAA and its own privacy policies in that it failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PHI of patients;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

[52] Change Healthcare Privacy Notice, *available at* https://www.changehealthcare.com/privacy-notice.

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain the security of protected health information, in violation of 45 C.F.R. § 164.530(b).

65. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data

security practices, which should be factored into all business-related decision making.[53]

66. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[54] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[55]

67. The FTC further recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[56]

---

[53] See *Start With Security: A Guide for Business*, Federal Trade Commission, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[54] *Id.*
[55] *Id.*
[56] *Id.*

68. Change Healthcare was fully aware of its obligation to implement and use reasonable measures to protect the PHI of the patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring.

PLAINTIFF'S CLASS ALLEGATIONS

69. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to the Federal Rule of Civil Procedure 23(b)(2), (b)(3), and (c)(4), on behalf of the following Class and Subclass (collectively, the "Class"):

Nationwide Class: All healthcare providers within the United States whose health insurance reimbursements payments were delayed or disrupted following UnitedHealth's announcement of the Data Breach on February 21, 2024.

New Jersey Subclass: All healthcare providers within New Jersey whose health insurance reimbursements payments were delayed or disrupted following UnitedHealth's announcement of the Data Breach on February 21, 2024.

70. Specifically excluded from the proposed Class are Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

71. Plaintiff reserves the right to modify or amend the foregoing Class and Subclass definitions before the Court determines whether certification is appropriate.

72. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23 because there is a well-defined community of interest in the litigation and membership in the proposed Class is readily ascertainable.

73. **Numerosity (Fed. R. Civ. P. 23(a)(1)).** The Class members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes over one million licensed healthcare providers. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

74. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3)).** Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to, the following:

a. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard the information systems targeted in the Data Breach;

b. Whether Defendants knew, or should have known, of the susceptibility of their information systems to cyberattacks;

c. Whether Defendants were negligent in maintaining, protecting, and securing their information systems;

d. Whether Defendants violated their duty to implement reasonable security systems to protect Plaintiff's and Class members' PHI;

e. Whether Defendants adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

f. Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

g. Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

h. Whether Defendants failed to comply with their own policies and applicable laws, regulations and industry standards relating to data security;

i. Whether Defendants failed to notify Plaintiff and Class Members as soon as practicable and without delay after the Data Breach was discovered;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to prevent or properly respond to the Data Breach;

k. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in losses;

l. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendants' conduct; and

m. Whether Plaintiff and Class members are entitled to relief, including damages and equitable relief.

75. **Typicality (Federal Rule of Civil Procedure 23(a)(3)).** Pursuant to Rule 23(a)(3), Plaintiff's claims are typical of the claims of the Class members. Plaintiff, like all Class members, suffered harm as a result of the Data Breach and ensuing shutdown of Defendants' computer networks.

76. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)).** Pursuant to Rule 23(a)(4), Plaintiff and its counsel will fairly and adequately protect the interests of the Class. Plaintiff has no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiff has retained counsel experienced in prosecuting class actions and data breach cases.

77. **Superiority (Fed. R. Civ. P. 23(b)(3)).** Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a

single adjudication, economy of scale, and comprehensive supervision by a single court.

78. While there are currently pending actions against defendants relating specifically to the Data Breach, healthcare providers have interests separate and apart from general users of Defendants' computer networks in that the Data Breach and related shutdown has affected healthcare providers' ability to receive payment of insurance claims for the medical treatment they provide. Thus, healthcare providers, such as Plaintiff, require representation related to their specific economic harm.

COUNT I

Negligence
(Against all Defendants))

79. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

80. Defendants had (and continue to have) a legal duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting confidential health and personal identifying information on their network systems. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated.

81. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between them and Plaintiff and Class

members, which is recognized by state and federal law, including but not limited to HIPAA. Only Defendants, however, were in a position to ensure that their computer networks were sufficient to protect against the harm to Plaintiff and the Class members that resulted from the Data Breach and ensuing shutdown.

82. Defendants owed a duty to Plaintiff and Class Members to timely disclose if their computer systems and data security practices were inadequate in any way, because such vulnerability or inadequacy would be a material fact in the decision to engage in business transactions with Defendants.

83. Defendants violated these duties and standards and duties by failing to exercise reasonable care in safeguarding and protecting PHI and PII on their network systems by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PHI and PII entrusted to them. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting PHI and PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in harm to Plaintiff and Class members.

84. Defendants knew or should have known of the inherent risks in failing to heed credible security warnings; failing to maintain adequate patch management policies and procedures; failing to detect alerts in regard to vulnerabilities affecting its systems; failing to properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; failing to properly use automated tools to track which versions of software were running and whether updates were available; and failing to implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities. Thus, Plaintiff and the Class Members were foreseeable and probable victims of Defendants' inadequate security practices and procedures.

85. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached their duties to Plaintiff and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting their data networks and PHI and PII within their possession, custody and control, which resulted in the shutdown of Defendants' computer networks and disrupted Plaintiff and Class members' businesses.

86. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached their duties to Plaintiff and

Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting PHI and PII.

87. But for Defendants' negligent breach of the above-described duties owed to Plaintiff and Class members, Defendants would not have experienced the Data Breach and would not have had to shut down the Change Healthcare networks, thereby preventing Plaintiff and Class members from (i) timely receiving insurance payments for previously submitted claims, (ii) submitting new insurance claims for payment, and (iii) obtaining insurance authorization for patient medical treatment, among other things.

88. The harms to Plaintiff and Class members were foreseeable given the types of services Defendants provide and the statutory obligations to protect their computer networks and confidential PHI and PII.

89. Defendants' wrongful actions, inactions, omissions, and want of ordinary care that directly and proximately caused the Data Breach and resulted in the shutdown of the Change Healthcare computer networks constitute negligence.

90. As a direct and proximate result of Defendants' wrongful actions, inactions, omissions, and want of ordinary care that directly and proximately caused the Data Breach and the related shutdown, Plaintiff and Class members have

suffered (and will continue to suffer) monetary losses and economic harms and seek all available damages.

COUNT II

Negligent Undertaking
(Against all Defendants)

91. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

92. By serving as an insurance claims clearinghouse and payment processor, Defendants undertook to render revenue and payment cycle management services that benefitted Plaintiff and Class members.

93. In undertaking to provide such services to Plaintiff and Class members, Defendants knew or should have known of the necessity to heed credible security warnings; maintain adequate patch management policies and procedures; detect alerts in regard to vulnerabilities affecting its systems; properly update and patch third-party software, update software regularly, implement third-party patches when issued, and prioritize patches by the severity of the threat; properly use automated tools to track which versions of software were running and whether updates were available; and implement appropriate procedures to keep security current and address vulnerabilities, including to monitor expert websites and software vendors' websites regularly for alerts about new vulnerabilities.

94. Only Defendants were in the position to ensure that their information systems, practices, and protocols were sufficient and consistent with industry standards and legal requirements.

95. Defendants failed to exercise reasonable care to perform these actions. Defendants failed to provide reasonable or adequate information systems and networks and failed to engage in appropriate cybersecurity practices to safeguard their claims processing and revenue cycle services.

96. Defendants' failure to fulfill their duties placed Plaintiffs and Class members in a worse position than they would have been had Defendants not undertaken such duties because other, more secure means would have been used to process insurance claims and payments for Plaintiff's and Class members' practices, which would have avoided the current disruption and lack of funds flowing to Plaintiff and the Class.

97. Defendants' failure to abide by their duties was wrongful and negligent in light of the foreseeable risks and known threats.

98. Defendants knew or should have known that failure to take appropriate actions to secure their systems increased the risk of harm to Plaintiff and the Class members beyond the risk of harm that existed without the undertaking.

99. As a direct and proximate result of Defendants' negligent undertaking, Plaintiff and the Class members have suffered and will suffer injury.

COUNT III

Negligent Failure to Warn
(Against all Defendants)

100. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

101. Upon information and belief, Defendants had been aware for a substantial period of time that their cybersecurity systems and networks were susceptible and prone to attack.

102. Defendants knew or should have known of their cybersecurity failures including, but not limited to, failing to heed credible cybersecurity warnings; and failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PHI and PII entrusted to them.

103. Nevertheless, Defendants failed to warn Plaintiff and Class members of the known cybersecurity vulnerabilities, failed to effectively remedy the cybersecurity flaws and problems in their systems and networks, failed to warn Plaintiff and Class members of likely risks caused by Defendants' failure to remedy such cybersecurity flaws, and failed to provide prompt notice to Plaintiff and Class members that the promised secure information systems had been breached by unauthorized persons during the Data Breach.

104. As a direct and proximate result of Defendants' negligent failure to warn, Plaintiff and the Class members have suffered and will suffer injury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all other members of the proposed Class, respectfully requests that the Court enter judgment against Defendants, and in favor of Plaintiff, as follows:

A. Certifying this action as a nationwide class action, appointing Plaintiff as representative of the Class, and designating his counsel as counsel for the Class;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages; statutory damages; consequential damages; punitive damages; exemplary damages; nominal damages; restitution; and disgorgement of all earnings, interest, profits, compensation, and benefits received as a result of their unlawful acts, omissions, and practices;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief as may be appropriate to protect the interests of Plaintiff and Class Members, including but not limited to an Order enjoining Defendants from engaging in the wrongful and unlawful conduct complained of herein;

D. Awarding Plaintiff and the Class pre-judgment and/or post-judgment interest as prescribed by law;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs and expenses as permitted by law; and

F. Granting such other or further relief in Plaintiff and the Class's favor as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury as to all issues so triable.

Dated: March 28, 2024

/s/ James E. Cecchi

CARELLA BYRNE CECCHI BRODY & AGNELLO, P.C.
James E. Cecchi
5 Becker Farm Road
Roseland, New Jersey 07068
T: (973) 994-1700
jcecchi@carellabyrne.com

GARDY & NOTIS, LLP
James S. Notis
Meagan A. Farmer
150 East 52nd Street, 11th Floor
New York, NY 10022
T: (212) 905-0509
jnotis@gardylaw.com
mfarmer@gardylaw.com

SQUITIERI & FEARON, LLP
Lee Squitieri
305 Broadway, 7th Floor
New York, NY 10007
T: (212) 421-6492
lee@sfclasslaw.com

Counsel for Plaintiff